



managed by Brookhaven Science Associates  
for the U.S. Department of Energy

# **SAFEGUARDS AND SECURITY MANAGEMENT SYSTEM EVALUATION**

**Submitted June 10, 2003**

***Facilitators:***      *Ray Costa, F&O Quality Program Coordinator*  
                                 *Eva Rothman, NSLS Training Coordinator*

***SAFEGUARDS & SECURITY MANAGEMENT SYSTEM:***

*Nancy W. Griffin, Division SBMS Coordinator* \_\_\_\_\_

*Russel J. Reaver, MS Point of Contact* \_\_\_\_\_

*Michael J. Bebon, MS Steward* \_\_\_\_\_

## **LIST OF ATTACHMENTS**

- |              |  |
|--------------|--|
| Attachment 1 | Safeguards & Security Evaluation Team Members                      |
| Attachment 2 | Safeguards & Security Management System Information Package        |
| Attachment 3 | Pre-Evaluation Workshop Meeting Presentation                       |
| Attachment 4 | Safeguards & Security Management System Evaluation<br>Presentation |

## EXECUTIVE SUMMARY

This evaluation was conducted to implement Critical Outcome 3.2.1.2 (Consensus based User/Peer Reviewer Maturity Determinations) and to support the Security Management Steward's desire and commitment to continually improve the operations of his management systems. The process used for the evaluation was established by the Office of Quality Programs and Services and has been used at BNL over the last several years. The process ~~reflects an approach similar to~~ ~~is based on the~~ Malcolm Baldrige ~~National Quality Award~~ criteria and evaluates the management system ~~in~~ ~~against~~ three ~~ways~~ criteria: ~~d~~Definition, ~~i~~Implementation, and ~~p~~Planning/~~a~~Assessment/~~i~~Improvement. The evaluation team consisted of 11 members representing science and technology, support organizations and the ~~e~~Offices of ~~i~~ntegrated ~~a~~Assessment and ~~e~~Counterintelligence. The Safeguards and Security DOE counterpart was invited but was unable to attend.

The results of the assessment indicated that the Safeguards and Security Management System was progressing well in the maturity process. Definition was rated at a 3 out of a possible 5, and ~~i~~Implementation and ~~p~~Planning/~~a~~Assessment/~~i~~Improvement both rated 4. The results of the evaluation do reflect that ~~i~~Implementation and ~~p~~Planning/~~a~~Assessment are appropriately a higher priority because of the ~~security concerns associated with~~ ongoing and sometimes rapidly changing ~~security~~ requirements.

A summary of strengths identified by the team is as follows:

- In spite of limited and overstressed resources, there is excellent identification, and efficient implementation, of rapidly changing information and requirements.
- Staff responsible for implementing security requirements prioritized the risks associated with implementation very well.
- There is an excellent self-assessment program that has resulted in decreased DOE required inspections of the Safeguards and Security Program.
- A Security Enhancements Plan exists to coordinate long-term security enhancements at the Laboratory. The Plan is updated annually.

The following opportunities for improvement were identified:

- Improve ~~communication of community access to~~ Material Control & Accountability requirements and procedures ~~to Laboratory population~~.
- Maintain legacy documents, such as the Security Manual, while converting them into Subject Areas.

- The casual visitor sticker process needs to be better coordinated with the Human Resources screening process.
- Determine the risk associated with inconsistencies in site access control procedures and operations.
- Improve the management of program performance expectations at the different levels (e.g., Area Office Manager, Deputy Area Office Manager, Contracting Officer) within the DOE Area Office.

These opportunities for improvement will be evaluated and a corrective action improvement plan developed. The ~~corrective action~~ improvement plan will be entered into ATS and tracked to completion.

## **INTRODUCTION**

The evaluation of the Laboratory's Safeguards & Security Management System (MS) that took place on May 21, 2003 served two purposes:

- Evaluate the performance of the Safeguards Security Management System as part of the Laboratory's Management System Assessment Planning initiative, and
- Provide the MS Steward and Point of Contact (POC) with information on the strengths and areas for improvement for the Management System.

This evaluation is part of Critical Outcome 3.2.1.2, Consensus-based User/Peer Reviewer Maturity Determinations, which is a contract performance measure for FY 2003. A Baldrige-based methodology was used to determine system/process maturity across three facets: **e**Definition; **i**Implementation; and **p**Planning, **a**Assessment & **i**Improvement. A Management System Evaluation Guide was included in the Information Package (Attachment 2).

## **SCOPE**

This evaluation focused on the safeguards and security key functions as defined and described in the Safeguards and Security Management System description of BNL's Standards Based Management System (SBMS) as well as its implementation throughout Laboratory organizations. The key purpose of the MS is to provide instruction and interpretation regarding protection of personnel, physical and intellectual property, and control and accountability of nuclear materials. Key Functions/Services and Processes of the MS are communicated in various ways: SBMS program descriptions, subject areas, interim procedures, and legacy documents; group-specific procedures; program specific committees; group-specific meetings; BNL website; Monday Memo's; and Lab-wide broadcast e-mails.

The SBMS areas that are currently assigned to the Safeguards and Security Management System are:

- Fraud, Waste, Abuse, Corruption, and Other Criminal Offenses Program Description
- SPI 5-01, Site Security Administration\*
- SPI 5-03, Classified Information & Security Requirements\*
- SPI 5-09, Unclassified Visits & Assignments of Foreign Nationals\*
- Security Manual\*

\* These legacy documents are included in a formalized plan for converting legacy documents to subject areas or other means of communication.

## **EVALUATION METHOD**

The evaluation method consisted of the following steps:

1. The process-Management System POC selected a representative team of stakeholders (Attachment 1).
2. The Safeguards & Security Division SBMS Coordinator POC developed and distributed an Information Package that contained a description of the processmanagement system, information about its operation, and data in the form of a presentation to be reviewed prior to the evaluation workshop (Attachment 2). The presentation was prepared in response to a standard set of questions provided by the Quality Programs & Services Office and organized to address the three criteria: Definition, Implementation, and Planning/Assessment & Improvement. The package was distributed May 9, 2003.
3. Team members reviewed the Information Package as well as their own internal data about the Safeguards and Security Management System in preparation for the Evaluation Workshop.
4. A pre-workshop meeting was held on May 16, 2003 to familiarize team members with the evaluation process and the criteria (Attachment 3).
5. The POC sponsored the Evaluation Workshop on May 21, 2003 to evaluate the Safeguards & Security Management System maturity in each area – Definition, Implementation, and Planning/Assessment & Improvement. Two experienced facilitators ran the workshop.
  - a. The facilitators presented the agenda, introductions, driver, objective and scoring information.
  - b. The Management System Steward presented an overview of the Critical Outcome measure and its relation to the workshop.
  - b.c. The POC presented an overview of the MS key functions/services and processes.
  - e.d. The Division SBMS Coordinator gave a presentation that discussed the purpose, overview and history of the MS (Attachment 4). The presentation was divided into three areas: Definition, Implementation, and Planning/Assessment Improvement.
  - d.e. The team used the Management System Evaluation Guide to score the process'-management system's maturity after each of the three sections of the presentation: Definition, Implementation, and Planning/Assessment Improvement.

e.f. The scoring process included a discussion/clarification of the information on the Safeguards & Security Management System pertinent to the criteria prior to the individual scoring. After the scoring, the team discussed the differences in individual scores and worked toward developing a consensus score. These discussions resulted in the identification of strengths and areas for improvement for the management system.

f.g. A closing discussion was held to gather feedback about the evaluation method.

g.h. A report documenting the evaluation was prepared for all team members as well as the MS POC and the MS Steward.

h.i. The MS Steward forwarded the report to the Deputy Director for Operations.

The evaluation team consisted of 11 members representing science and technology, support organizations, the integrated assessment program, and the Counterintelligence Office. The Safeguards and Security DOE counterpart was invited, however was unable to attend. All members spent time reviewing the Information Package provided by the Safeguards and Security SBMS Coordinator. Those who were not familiar with the evaluation process attend the Pre-Workshop meeting. One observer was present from the Safety & Health Services Division.

## **RESULTS**

The Safeguards and Security Management System was found to be positively progressing inthrough the maturity process. Definition was rated at a 3 out of a possible 5. Although key functions are outlined in the management system description, progress on converting the legacy documents associated with the MS has been hampered by limited resources for development, review, approval and publication. Though there was some disagreement by the evaluators with respect to its merit, SBMS guidelines allow processes that apply to small groups to be communicated in ways other than subject areas. The Safeguards and Security Management System, which serves many small groups, has implemented these requirements through other means, i.e. classified computer security requirements are communicated through a Master Information System Security plan to users with annual training, classification of documents is implemented through annual-periodic training sessions and DOE classification guides, and requirements for classified areas are implemented through specific physical protection plans. A Proposal for Conversion of Legacy Documents was prepared and presented to the SBMS Steering Committee in May 2002. Progress has been made on the actions outlined in this Proposal, however some legacy documents have not been kept up-to-date during the interim.

Implementation and Planning/Assessment/Improvement were both rated 4. This reflects the importance placed on analyzing and communicating security concerns and changes in requirements in the most expedient way to the Laboratory community. Although a formal survey had not been conducted up to now, line organizations have been asked to complete a safeguards and security self-assessment designed to provide the MS Steward with strengths and improvement opportunities for the management system.

Much discussion revolved around the SBMS process. It was the consensus that the SBMS process for getting documents created/updated/approved is currently cumbersome and time consuming thereby holding back forward progress.

Some DOE safeguards and security requirements are changing so fast that it is difficult to develop and implement an immediate official policy/procedure that would be in effect long before completion of the process it takes to publish it officially. Currently, memos, e-mails, verbal communications, and interim procedures (as well as departments themselves keeping their staff/users informed) have gotten the job done admirably in terms of getting the word out in real time, but this still leaves no single centralized place to go to for up-to-date information should there be a need to consult the latest policy or procedures afterward. Even with up-to-date, easily accessed information, there will still be problems and confusion because of "information overload." There is so much rapidly changing information that is not only difficult to track and keep the community familiar with, there is also a tendency to ignore what is being communicated altogether.

Another point—observation brought out at the workshop involved downward communications. It was found that information communicated to Level I/II Management is not always forwarded down to Administrators and Level I/II Assistants. Dept/Div Administrators, more often than not, are the ones responsible for coordinating implementation of new and updated processes and procedures and quite often they are left out of the information loop. (Note: This was a general observation not specifically directed at the Safeguards and Security management system. The MS POC pointed out that he includes Level I/II Assistants when distributing information to Level I/II managers.)

The evaluation workshop results are summarized in the following table. Each asterisk represents an individual team member's score.

Scoring			
Rank	Definition	Implementation	Planning/Assessment/ Improvement
5 (High)		*	
4		*****	*****
3	*****	*	
2	*		
1 (Low)			

**Discussion – Definition**

The majority ranked this criterion at 3 with one member ranking at 2 – consensus at 3.

***The following Areas for Improvement were noted:***

1. Information regarding the Material Control & Accountability process was not easily found on the SBMS due to being fragmented and located within several areas of the SBMS.
2. The Security Manual, a legacy document on the SBMS, is not currently up-to-date and does not provide current policy and procedures for use by the Lab population. The Proposal for Conversion of Legacy Documents addresses the Security Manual, however, there needs to be an evaluation to determine if updates should be made to legacy documents until the conversion is complete.

***The following Strengths were noted:***

1. In spite of limited resources within the Division, there is excellent identification of rapidly changing requirements and communication of this information to all levels of the Laboratory.
2. An excellent job is done in identifying and mitigating risks to BNL, i.e., as evidenced by the Unclassified Foreign Visits & Assignments Program, the Classified Information Security Program, and the Physical Security Program.

**Discussion – Implementation**

The majority of rankings were 4, with one member ranking at 3 and one member ranking at 5 – consensus at 4.

***The following Areas for Improvement were noted:***

1. DOE funding for Safeguards and Security is not currently adequate and direct funding is not effectively working at the science labs. This is a DOE issue.
2. ~~The C~~casual visitor sticker process sometimes enables people to bypass Human Resources check-in requirement and screening process.
3. There have been inconsistencies with the gate access control procedures and operations. Need to evaluate the cause of the inconsistencies, determine the risk to the Lab, and implement any corrective actions deemed appropriate.

***The following Strengths were noted:***

1. Despite limited and overstressed resources in some of the program areas, implementation of changing requirements is extremely efficient.
2. Staff responsible for implementing security requirements prioritize the risks associated with implementation in an efficient and effective manner.
3. Services are successfully oriented towards primary customers: DOE and Lab population
4. There is strong coordination of effort with other Lab organizations to communicate, explain, and implement new requirements.

**Discussion – Planning/Assessment/Improvement**

All members of the evaluation team ranked this area at 4.

***The following Areas for Improvement were noted:***

1. Improve~~ment is needed in~~ the management of program performance expectations ~~through enhanced communications within~~ the different levels in the DOE Area Office (BAO).

Note: Currently, the BAO security representative has an excellent working relationship with the Safeguards and Security Division and this area of improvement

does not reflect on the performance of this relationship, but will serve to enhance it as well.

***The following Strengths were noted:***

1. There is an excellent established self-assessment program. DOE inspections are only conducted every two years, instead of annually, due to the strength of the self-assessment program and continuing satisfactory inspection ratings.
2. DOE inspection ratings continue to be high with the exception of the Unclassified Foreign Visits and Assignments (FVA) Program. Currently, the Laboratory is in compliance with the FVA requirements and has completed and submitted an inspection status report to DOE Headquarters requesting closure of all findings.
3. A Security Enhancements Plan coordinates long-term security enhancements at the Laboratory. The plan is updated annually for tracking progress and establishing other short and long-term activities.

**CONCLUSION**

This evaluation achieved both objectives. The performance of the Safeguards Security Management System was reviewed. The results indicated ample system effectiveness with specific areas for improvement.

As a result of this evaluation, the MS Steward and Point of Contact (POC) have information that will lead to improvements of the Management System.

The MS Steward and POC have committed to developing an action item list to address the Areas of Improvement. These corrective-improvement actions will be entered into ATS and tracked to completion.~~tracked in the F&O Corrective Action Tracking database.~~